# OA/ITSD Information Security Management Office
## Monthly Cyber Security Tips
# NEWSLETTER

**OCTOBER 2006**                                              Volume 1, Issue 5

## Top Ten Cyber Security Tips

**October is National Cyber Security Awareness Month.**

In recognition of Cyber Security Awareness Month, this edition of the newsletter is designed to remind people of the TOP 10 simple, easy, and basic things that everyone can and should do to protect their computer systems and data from harm by various cyber attacks and other types of security incidents that can cause damage, consume computer resources, or expose confidential information.

**1.   Use and regularly update firewalls, anti-virus, and anti-spyware programs.**

There are many types of Internet security and safety issues that you should defend against.  One of the most effective ways of defending your computer is to use a firewall and up to date anti-virus and anti-spyware products.

A **firewall** works by filtering information coming from and going to your network/computer and/or the Internet. It identifies and rejects information that comes from a location or source known to be dangerous or contains information that seems suspicious. **Anti-Virus** programs can stop Viruses, worms, and Trojan horses, which are malicious programs that can cause damage to your computer and information on your computer. Those malicious programs can also slow down the Internet access and might even use your computer to spread themselves to your friends, family, or co-workers.  Spyware is a general term used for software that performs certain behaviors such as pop-up advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent. An **anti-spyware** program helps stop such misuse, but  they need to be kept up to date in order to detect the newest identified threats as well. Configuring your anti-virus and anti-spyware products to automatically update their identification files on a daily basis is highly recommended.

> For more information visit:
> http://www.msisac.org/localgov/info/firewall-guide.pdf
> http://www.msisac.org/awareness/oct05/csab05.pdf
> http://www.staysafeonline.com/toolbox/fundamentals/defend_yourself.html
> http://www.us-cert.gov/cas/tips/ST04-005.html
> http://www.us-cert.gov/cas/tips/ST04-016.html

**2.   Properly setup and patch operating systems, browsers, and other software programs.**

Whenever security updates or service packs become available for your operating system or programs, it is very important to promptly download them and patch your operating systems and programs.  These patches are created to protect systems against potential attacks.  Be awre that attacks sometimes occur before updates are released. Make sure you update any software you use for browsing the Internet (Internet Explorer, Firefox, Netscape, Opera, Amaya, etc.) because Internet-based browsing attacks are

becoming more common and more dangerous.  Other software programs that communicate or interact with the Internet, like e-mail, Web servers, and remote desktop software are especially susceptible to attacks and should be kept current on patches and version levels.

For more information visit:
http://www.msisac.org/awareness/oct05/csab05.pdf
http://www.us-cert.gov/cas/tips/ST05-001.html
http://www.staysafeonline.com/toolbox/fundamentals/keep_up-to-date.html

3.  **Passwords and authentication methods.**

Passwords and other authentication methods are ways systems verify that you are who you claim to be. If someone authenticates as you, the system will think it's you.  That person can do anything you can do on your computer and the system will log their actions (such as deleting files, sending malicious e-mails, or browsing to inappropriate sites) under your access credentials.  Don't share your passwords and access codes, don't store them in unencrypted files, and don't write them down unless you then place them in a locked, secured location.  Default passwords, names and dictionary words, even in different languages, can be easily guessed or cracked so use complex passwords that are at least eight characters long and have numbers, letters, and special characters in them.  Passwords aren't much use if you cannot remember them, so use a pass-phrase instead.  The phrase "Would you like 3 scoops of ice cream?" can become the strong password "Wul3$o1c?"

For more information visit:
http://www.msisac.org/awareness/oct05/csab05.pdf
http://www.microsoft.com/athome/security/privacy/password.mspx
http://www.us-cert.gov/cas/tips/ST04-002.html

4.  **Lock your workstation/laptop when you leave it and configure it to automatically lock after a short period of inactivity.**

One of the fastest ways to compromise a system is to simply walk up to an unattended, unlocked workstation or server and access the system so be safe and lock your system when you leave it. It's also very easy to get sidetracked and stay away from your desk longer than you anticipate so configure your system to automatically lock after a short period of inactivity. It is an easy way to help protect your account and the items you have access to. Lockout after fifteen minutes of inactivity is recommended and shorter periods for critical systems.

For more information visit:
http://www.msisac.org/awareness/oct05/csab05.pdf
http://www.us-cert.gov/cas/tips/ST04-003.html

5.  **Backup important files regularly.**

There are many ways you can lose information on a computer – a destructive virus, a power surge, lightning, floods, a big magnet, or sometimes equipment just fails.  If you regularly make backup copies of your files and keep them in a separate place, you can get some, or even all, of your information back in the event something happens to the originals on your computer.

For more information visit:
http://www.msisac.org/awareness/oct05/csab05.pdf
http://www.staysafeonline.com/toolbox/fundamentals/backup_basics.html
http://www.us-cert.gov/cas/tips/ST04-003.html

6.  **Be cautious when using the Internet.**

Browsing to non-work related sites can increase the risk of becoming infected with spyware, viruses and other malicious code.  Download files and install programs only when you are authorized to do so, and only when there is a real need.  Know with whom you are dealing on the Internet – anonymous doesn't

necessarily mean safe, and many criminals are very good at impersonating real financial organizations like banks and credit card companies.  Never share personal or confidential information if you are not the initiator of the transaction.  Never share sensitive or confidential information over an unencrypted Internet connection.

> For more information on safe browsing tips visit:
> http://www.msisac.org/awareness/oct05/csab05.pdf
> http://www.us-cert.gov/cas/tips/ST04-013.html
> http://www.us-cert.gov/cas/tips/ST04-012.html

### 7.  Messaging security – e-mail and instant messaging.

E-mail and instant messaging (IM) are wonderful tools but they can be used or misused in a variety of ways.  Do not send confidential or sensitive information, like Social Security numbers, account numbers, or secret information through unencrypted e-mail or IM.  Do not open a message or an attachment from an unknown sender.  If you share personal information with others as a result of answering spam or phishing messages, your identity can also be stolen.

> For more information visit:
> http://www.microsoft.com/athome/security/email/attachments.mspx
> http://onguardonline.gov/phishing.html
> http://www.consumer.gov/idtheft/ddd/index.html
> http://hoaxbusters.ciac.org/

### 8.  Review your computer security.

Evaluate your computer's security periodically and apply appropriate repairs, upgrades, and replacements.  If you don't maintain your system's security by keeping it up-to-date, it will eventually be exposed to serious security threats.

> For more information visit:
> http://www.staysafeonline.com/toolbox/how_to/index.html

### 9.  Responding to a cyber incident.

Learn how to recognize cyber attacks and know what to do if things go wrong.  Ask if your organization has a cyber security incident response plan and a cyber security incident response team and use it when appropriate.  Remember that rapid response can be crucial, so when things do go wrong or you encounter a suspicious security-related event, report it immediately.  If you don't know how to report a cyber incident, ask someone in your IT department or your help desk.

### 10. Remember that cyber security is everyone's responsibility.

Just like one leak can sink a boat, one data leak, one security breach, or one malicious worm can sink an organization.  By protecting yourself and the systems entrusted to you, you are protecting your co-workers, your entire organization's network and data and, ultimately, the citizens who are depending on you.

**Brought to you by:**                                    http://www.msisac.org